UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/057,914	01/29/2002	Jens-Peter Redlich	A7995	3714

7590 07/13/2005

SUGHRUE MION, PLLC
2100 Pennsylvania Avenue NW
Washington, DC 20037-3213

EXAMINER	
PATEL, CHIRAG R	
ART UNIT	**PAPER NUMBER**
2141	

DATE MAILED: 07/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/057,914	REDLICH ET AL.	
	Examiner	Art Unit	
	Chirag R. Patel	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Arguments

Applicant's arguments filed for claims 1-35 have been fully considered but they are not persuasive.

As per claim 1, applicant argues:

a) Specifically, the present invention (as recited in claim 1) requires establishing an association between a terminal and an untrusted access station. Giniger does not discloses nor suggest establishing such an association between a terminal and an untrusted access station.

Examiner's Response:

Per the disclosure, the applicant states per [0033] & [0044] the definition of an access point "A refers to an access station. An access station is used to connect a terminal device U to an IP-based infrastructure network, e.g. Intranet or Internet. It receives traffic from the IP network and delivers it to the correct terminal U, and, it receives traffic from terminals U and forwards it to the IP network."

Giniger et al. discloses per Col 9 lines 30-56, and Figure 2 "An Internet Point-of-Presence (POP) 220 provides an access point for communication between edge device 110 and Internet 100. In particular, customer premises 220 are coupled to POP 220 by a communication link 216. In this first example, communication link 216 is a dedicated communication link, such as a T-1 or T-3

digital service leased from a telephone carrier. Edge device 110 is connected to computers 120 over a local area network link 208, such as an Ethernet link which forms part of subnetwork 125. A communication interface, such as a DSU/CSU, couples edge device 110 to communication link 216. At POP 220, a corresponding communication interface 222 is also coupled to communication link 216 and communication interface 222 is coupled to a router 226, which provides a communication interface with Internet 110. Communication links 212, 214, and 224, which pass communication between edge device 110 and router 226 in general carry communication for multiple tunnels 115, communication between edge device 110 and management server 130, and other IP-based communication to computers and other devices coupled to it over Internet 100. That is, referring back to FIG. 1, individual tunnels 115 and communication links 135 are all carried over a common physical communication link 216 (FIG. 2)."
By reading the claims in light of the specifications, the POP "An Internet Point-of-Presence (POP) 220" reads on the definition of an access station as provided by the applicant. The link 216 is the association between the edge device and the POP 220. The POP 220 connects a user terminal device to an IP-based infrastructure network.

b) Giniger does not diosclose (or suggest) establishing an association with an untrusted access station. The Examiner appears to read the untrusted access station on the edge devices 110(See 9:30-35 of Giniger). However, there is no

disclosure (or suggestion) that one or more of these edge devices are untrusted.

Examiner's Response: Per the above discussion, POP "An Internet Point-of-Presence (POP) 220" reads on the definition of an access station as provided by the applicant. Per column 6 lines 14-22, Giniger et al. discloses "The communication system provides comprehensive security to guarantee the safe transmission of mission-critical data over public networks. In addition to the secure encryption and authentication of content, the protocols and processes used to manage node devices from a central server are also secure. The control information exchanged between management server(s) and VPN devices is securely authenticated, encrypted, and protected from replay and other spoofing attacks."

As per claim 4, applicant argues:

a) Further, claim 4 requires that the packets flowing between the terminal and the trusted network element be transmitted via the untrusted access station.

Examiner's Response:

Please see discussion under claim 1.

As per claim 5, applicant argues:

a) Claim 5 requires the secure tunnel to enable the ISP to dynamically obtain

control of resources in the untrusted access station. There is no disclosure (or suggestion) for a secure tunnel between the edge devices of Giniger to be able to control the resources of another end node.

Examiner's Response:

Giniger et al. discloses per Col 11 lines 55-58 and Figure 4 "A key exchange module 410 is used to exchange cryptographic keys with other computers or devices on Internet 100 in order to establish secure tunnels with those computers or devices." Giniger discloses per column 8 lines 29-41 " Each edge device 110 securely communicates with a management server 130. Management server 130 is responsible for directing edge devices 110 to establish tunnels 115 among one another, and otherwise controlling their operation. This control includes authenticating the edge devices, and providing information to the edge devices that the edge devices use to establish particular secure communication tunnels 115. For example, management server 130 provides session keys to the edge devices for use in encrypting communication passing through particular tunnels. In this way, management server 130 can limit which edge devices 110 can enter into a VPN, and in particular, can prevent edge devices 110 that it cannot authenticate from entering the VPN."

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 1-22, 24-25, 28, 30, 33 and 35 are rejected under 35 U.S.C. 102(e) as being anticipated by Giniger et al. (US 6,751,729).

As per claim 1, Giniger et al. discloses a method for performing mutual authentication and authorization of a user's terminal device (U) and an Internet Service Provider (P) (Col 11 lines 55-58) in order to establish secure communication between the terminal (U) and a trusted network element (T) to the Internet via an untrusted access station (A) comprising:

establishing an association between a terminal (U) and an untrusted access station (A); (Col 9 lines 30-35)

transmitting an ISP authentication packet from terminal (U) to ISP (P) via the untrusted access station (A); (Col 14 lines 47-50)

sending a user authentication packet from said ISP (P) to said terminal (U) via said untrusted access station (A); (Col 8 lines 36-41)

upon authentication of said terminal (U) and said ISP (P), said ISP performs the following: generating a session key; (Col 15 line 19)

distributing said session key to said terminal (U) and a trusted network element (T), wherein said session key is used to encrypt traffic between the terminal (U) and the trusted network element (T); (Col 15 lines 19-22)

establishing a secure tunnel such that the terminal (U) may communicate with the Internet via said trusted network element (T); wherein said secure tunnel emulates a physical link between the terminal (U) and the trusted network element (T) (Col 11 lines 55-58) such that traffic transmitted between the terminal (U) and said Internet via said trusted network element (T) is secure from modification or eavesdropping by said third party access station (A). (Col 12 lines 14-22, Col 6 lines 14-22)

As per claim 2, Giniger et al. discloses the method for performing mutual authentication and authorization of a terminal (U) and an Internet Service Provider (P) in order to establish a secure tunnel between the terminal (U) and a trusted network element to the Internet (T) via an untrusted access station (A) of claim 1, wherein the ISP (P) authentication packet contains an authentication challenge (CH_U) from terminal (U) to ISP (P) to authenticate the identity of ISP (P). (Col 5 lines 62-65, Col 12 lines 15-17, Col 12 lines 25-27, Col 14 lines 57-62)

As per claim 3, Giniger et al. discloses the method for performing mutual authentication and authorization of a terminal (U) and an Internet Service Provider (P) in order to establish a secure tunnel between the terminal (U) and a trusted network element to the Internet (T) via an untrusted access station (A) of claim 1, wherein the user authentication packet contains an authentication challenge (CH_P) from ISP (P) to the terminal (U) to authenticate the identity of user (U). (Col 5 lines 58-67, Col 12 lines 25-27, Col 14 lines 52-57)

As per claim 4, Giniger et al. discloses a method for providing public access to IP-based networks via an untrusted infrastructure having untrusted access points comprising:

establishing a connection between an IP-device (U) and said untrusted access point (A), (Col 9 lines 30-35, Figure 2 item 220) wherein an IP address is dynamically allocated to said IP device; (Col 11 lines 59-63)

transmitting an ISP authentication request from said IP device (U) to an internet service provider (P) affiliated with said IP device (U), (Col 14 lines 47-50) wherein said authentication request is transmitted through said untrusted access point (A) affiliated with said untrusted third party owned infrastructure; (Col 9 lines 30-35, Figure 2 item 200)

transmitting a user authentication request from said ISP (P) to said IP device (U) to determine whether said IP device (U) is a valid user affiliated with said ISP (P), (Col 8 lines 36-41) wherein said authentication request is transmitted through said untrusted

access point (A) affiliated with said untrusted third party owned infrastructure; (Col 9 lines 30-35, Figure 2 item 200)

when said ISP (P) authentication request and said user authentication requests is affirmative, (Col 14 lines 54-67) said ISP (P): generates a key session for encrypting data packets; and distributes said session key to said IP device (U) and a trusted node (T), wherein said session key is used to encrypt data transmitted between said IP device (U) and said trusted node (T); (Col 15 lines 19-22)

establishing a secure tunnel (Col 11 lines 55-58) as said session key is used to encrypt data packets transmitted between said IP device (U) and said trusted node (T), such that said data packets transmitted between said IP device (U) and an Internet via the untrusted access station (A) are protected from modification and manipulation by said untrusted access station (A) in said secure tunnel. (Col 12 lines 14-22, Col 6 lines 14-22)

As per claims 5, 6 and 35, Giniger et al. discloses a method for providing public access to IP-based networks through a third party owned, untrusted infrastructure having untrusted access stations (A) comprising:

establishing a connection between an IP-device (U) and said access station (A), (Col 9 lines 30-35) wherein an IP address is dynamically allocated to said IP device (U); (Col 11 lines 59-63) sending an ISP authentication request to said internet service provider (P) affiliated with said IP device (U) requesting to validate the authenticity of the ISP (P); (Col 14 lines 47-50, Col 14 lines 57-62)

sending a user authentication request from said ISP (P) to said IP device (U) to validate whether said IP device (U) has a service agreement with said ISP (P); (Col 14 lines 47-54) upon affirmative authentication of said ISP (P) and said IP device (U); (Col 14 lines 54-57)

establishing a trusted connection between said IP device (U) and a trusted network element (T), (Col 11 lines 55-58) wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in (Col 16 lines 41-46) said untrusted third party owned access station (A) (Col 9 lines 30-35, Figure 2 item 200) in order to provide the IP device (U) with prescribed for services. (Col 10 lines 9-20)

As per claim 7, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the ISP authentication request contains an authentication challenge (CH_U) from terminal (U) to ISP (P) to authenticate the identity of ISP (P). (Col 5 lines 62-65, Col 12 lines 15-17, Col 12 lines 25-27, Col 14 lines 57-62)

As per claim 8, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the user authentication request contains an authentication challenge (CH_IP) from ISP

(P) to the terminal (U) to authenticate the identity of terminal (U) as having subscribed to said ISP (P) for services. (Col 5 lines 58-67, Col 12 lines 25-27, Col 14 lines 52-57)

As per claim 9, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, the ISP (P) generates a session key for encrypting data packets upon the affirmative authentication of the terminal (U) and the ISP (P). (Col 14 lines 54-67, Col 15 line 19-22)

As per claim 10, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the ISP (P) selects a trusted node (T) with said Internet. (Col 16 lines 42-45, Col 17 lines 24-28)

As per claim 11, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 9, wherein said ISP (P) distributes said session key to the terminal (U) and the trusted node (T). (Col 15 lines 19-22)

As per claim 12, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the session key is used to encrypt data packets transmitted between the terminal (U) and the trusted node (T). (Col 15 lines 19-22)

As per claim 13, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 12, wherein the transmission of encrypted data packets between the terminal (U) and the trusted node (T) established a secure tunnel. (Col 11 lines 55-58)

As per claim 14, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 13, wherein the secure tunnel protects the data packets from manipulation by said untrusted access station (A). (Col 12 lines 14-22, Col 6 lines 14-22)

As per claim 15, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, a time out

is distributed to the trusted node (T) and terminal (U) upon the establishment of a secure tunnel. (Col 6 lines 23-27, Col 17 lines 28-34)

As per claim 16, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 15, wherein the timeout value is set to a predetermined time period, wherein if the secure tunnel is active for a time period equal to the timeout value, the secure tunnel will expire and the resources utilized for the secure tunnel will be releases. (Col 6 lines 23-27, Col 17 lines 28-34)

As per claim 17, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein upon receipt of an encrypted data packet from the terminal (U), the trusted node (T) decrypts the data packet and forwards the decrypted data packet to the Internet. (Col 7 lines 45-48, Col 12 lines 19-22, Col 15 lines 19-22, Col 17 lines 44-47)

As per claim 18, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 17, wherein upon receipt of an encrypted data packet from the terminal (U), the trusted node (T)

decrypts the data packet and forwards the decrypted data packet to a remote communication peer (R). (Col 12 lines 19-22, Col 15 lines 19-22, Col 17 lines 44-47)

As per claim 19, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 18, wherein the Internet sends an original data packet to the terminal (U) via the trusted node (T), wherein the trusted node (T) encrypts the original data packet and forwards the encrypted data packet to the terminal (U) via the untrusted access station (A). (Col 9 lines 30-35, Col 12 lines 19-22, Col 15 lines 19-22, Col 17 lines 44-47)

As per claim 20, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 17, wherein upon receipt of the encrypted data packet from the trusted node (T), the terminal (U) utilizes the session key to decrypt the data packet thus yielding the original data packet from the Internet. (Col 13 lines 54-59, Col 15 lines 44-47, Col 17 lines 44-47)

As per claim 21, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 18, wherein a remote communication peer (R) sends an original data packet to the terminal (U) via

the trusted node (T), wherein the trusted node (T) encrypts the original data packet and forwards the encrypted data packet to the terminal (U) via the untrusted access station (A). (Col 9 lines 30-35, Col 12 lines 9-12, Col 15 lines 9-12, Col 17 lines 44-47)

As per claim 22, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 21, wherein upon receipt of the encrypted data packet from the trusted node (T), the terminal (U) utilizes the session key to decrypt the data packet thus yielding the original data packet from the remote communication peer (R). (Col 13 lines 54-59, Col 15 lines 44-47, Col 17 lines 44-47)

As per claim 24, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the untrusted access station (A) is incorporated into a third party owned network infrastructure. (Col 9 lines 30-32)

As per claim 25, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 24, wherein

the ISP (P) provides the terminal (U) with at least one subscribed for service via an untrusted access station (A). (Col 10 lines 9-20)

As per claim 28, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 24, wherein the untrusted access station (A) is located in the network infrastructure of a public facility. (Col 6 lines 14-16, Col 10 lines 9-20)

As per claim 30, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 24, wherein the untrusted access station (A) is located within the infrastructure of a private household or within the private infrastructure of a corporation or government institution. (Col 6 lines 44-46, Col 10 lines 9-20)

As per claim 33, Giniger et al. discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the terminal (U) recognizes a compatible access point by broadcasting a dynamic host configuration protocol (DHCP) request and receiving a "magic" DHCP response from

the untrusted access station (A). (Col 9 lines 5-11, Col 11 lines 36-51, Col 11 lines 59-67, Col 12 lines 1-2)

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 23, 26-27, 29, 31-32 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Giniger et al. (US 6,751,729) in view of Rueda et al. (US2002/0112076).

As per claim 23, Giniger et al. discloses a method of claim 6, however, fails to disclose providing an accounting of time to the untrusted access station (A) for resources utilized by the terminal (U). Rueda et al. discloses wherein the ISP (P) provides an accounting of time to the untrusted access station (A) for resources utilized by the terminal (U). ([0202]) It would have been obvious to a person of ordinary skill in the art at the time the invention to provide an accounting of time to the untrusted access station (A) for resources utilized by the terminal (U) in the disclosure of Giniger et al. because it allows for proprietors of the system to bill for usage. ([0188])

As per claim 26, Giniger et al. discloses a method of claim 6, however, fails to disclose that the ISP (P) reimburses the untrusted access station (A) for resources expended on the terminal (U) according to an accounting of time. Rueda et al. discloses wherein the ISP (P) reimburses the untrusted access station (A) for resources expended on the terminal (U) according to an accounting of time. ([0189], [0202]). It would have been obvious to a person of ordinary skill in the art at the time the invention for the ISP (P) to reimburse the untrusted access station (A) for resources expended on the terminal (U) according to an accounting of time in the disclosure of Giniger et al. because it is an excellent opportunity for advertisement and provide branding, services, and advertising messages to users. ([0189])

As per claim 27, Giniger et al. discloses a method of claim 25, however, fails to disclose the ISP (P) bills the terminal (U) for services provided to the terminal (U). Rueda et al. discloses wherein the ISP (P) bills the terminal (U) for services provided to the terminal (U). ([0188]) It would have been obvious to a person of ordinary skill in the art at the time the invention for the ISP (P) to bill the terminal (U) for services provided to the terminal (U) in the disclosure of Giniger et al. because it allows to charge costs incurred by the visiting client for system services. ([0200])

As per claim 29, Giniger et al. discloses a method of claim 28, however, fails to disclose the public facility is at least one of an airport, a convention center, a restaurant, a hotel, a library, and a school. Rueda et al. discloses wherein the public facility is at

least one of an airport, a convention center, a restaurant, a hotel, a library, and a school. ([0063],[0153]) It would have been obvious to a person of ordinary skill in the art at the time the invention for a public facility to be an airport, a convention center, a restaurant, a hotel, a library, and a school in the disclosure of Giniger et al. because it allows travelers would be able to have high-speed Internet access from within their suites with their computers that have been configured for their individual corporate LANs or home use. ([0063]).

As per claim 31, Giniger et al. discloses a method of claim 6, however, fails to disclose the untrusted access stations (A) is compatible with at least one wireless transmission. Rueda et al. discloses wherein the untrusted access stations (A) is compatible with at least one wireless transmission standard including WLAN (IEEE 802.11), BlueTooth (IEEE 802.15), or HiperLan. ([0267],[0268]) It would have been obvious to a person of ordinary skill in the art at the time the invention for the untrusted access stations (A) to be compatible with at least one wireless transmission because it provides laptop access using wireless lan cards. ([0268])

As per claim 32, Giniger et al. discloses a method of claim 6, however fails to disclosure the terminal (U) is a mobile device. Rueda et al. discloses wherein the terminal (U) is a mobile device. ([0063], [0207], [0274]) It would have been obvious to a person of ordinary skill in the art at the time the invention for the terminal (U) to be a mobile device in the invention of Giniger et al. because more and more business

transactions are initiated, negotiated and closed with no concern for geography. ([0063])

As per claim 34, Giniger et al. discloses a method of claim 6, however, fails to disclose the assigning a local unique identification (LUID) to the terminal (U) in order to facilitate matching the terminal with data packets. Rueda et al. discloses wherein the untrusted access station (A) assigns an local unique identification (LUID) to the terminal (U) in order to facilitate matching the terminal with data packets when the untrusted access station (A) is simultaneously serving multiple terminals (U). ([0135]-[0136], Figure 14). It would have been obvious to a person of ordinary skill in the art at the time the invention to assign a local unique identification (LUID) to the terminal (U) in the disclosure of Giniger et al. because it allows a server system to send a packet back to the correct client when two or more clients have the same IP address. ([0134])

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. These references are disclosed in the Notices of References cited page and teach numerous ways of implementing a multi-ISP controlled access to IP networks, based on third party operated untrusted access stations. A close review of these references is recommended.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chirag R. Patel whose telephone number is (571)272-7966. The examiner can normally be reached on Monday to Friday from 7:30AM to 4:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia, can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER